UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/469,726	12/21/1999	XIN WANG	D/99164	5313

7590 10/31/2006

MARC S. KAUFMAN
NIXON PEABODY LLP
8180 GREENSBORO DRIVE
MCLEAN, VA 22102

EXAMINER
HA, LEYNNA A

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/469,726	Applicant(s) WANG, XIN	
	Examiner LEYNNA T. HA	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 August 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-22 is pending.

2. This is a Non-Final rejection.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 7, 2006 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-8, 10-20, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright, et al. (US 6,084,969), and further in view of Jakobsson (US 6,587,946).**

As per claim 1:

Wright, et al. disclose a method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising the steps of:

generating a session key based on a random number **[col.11, lines 46-50]** privately maintained by only the owner, including the encryptor **[col.9, lines 51-52]**, of the original document; **[col.5, lines 2-4 and col.7, lines 10-11]**

encrypting the original document with the session key to create an encrypted document; **[col.5, lines 21-22 and col.7, lines 12-13]**

generating a proxy key based on a public key **[col.10, lines 26-28 and col.11, line 11]** corresponding to the selected recipient; and **[col.11, lines 65-67 and col.14, lines 35-36]**

transforming the encrypted document with a proxy key to create a transformed document **[col.14, lines 65-67]**, wherein the encrypted document remains in an encrypted state **[col.12, lines 55-56]** during the transformation to the transformed document.

Wright discloses alternative methods for secure message transmission. There is a method that decrypts and then re-encrypts the message and there is the alternative method of a straight through process of the encryption and the re-encryption process throughout the transformation of the encrypted document where the encryption remains encrypted **[col.13, lines 49-65 and col.14, lines 16-30]**. It is obvious that a message being encrypted is considered a message that has been transformed. However, Wright did not explain the encrypted message transforms to the encrypted message into a transformed message that is not decrypted to the original message and re-encrypted.

Jakobsson teaches proxy cryptography and demonstrates that asymmetric proxy transformations exist (col.3, lines 18-21). Jakobsson discloses the asymmetric encryption where the transformation is performed under quorum control, which guarantees that if there is not a dishonest quorum, then the plaintext message whose encryption is being transformed is not revealed to the proxy servers. Jakobsson's solution is efficient allowing tight control over actions and forwarding secret key encrypted messages from a primary recipient to a secondary recipient without disclosing the underlying encrypted message (col.3, lines 50-63). Jakobsson discloses the proxy transforming encrypted messages to encryptions with a variety of different recipient public keys to allow for categorization of the encryptions (col.4, lines 17-20). Further, Jakobsson includes the proxy to transform an encryption which the proxy could not decrypt into an encryption for which the proxy holds the secret key (col.6, lines 10-14). It would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of Wright with transforming the encrypted message to a transformed message that is not decrypted and re-encrypted as taught by Jakobsson because during transformation the plaintext is not revealed which leads to not being decrypted and transforming an encrypted message is efficient and does not disclose the underlying encrypted message (col.3, lines 50-63).

As per claim 2: See Wright on col.14, lines 65-67; discusses transforming the transformed document to the selected recipient.

As per claim 3: See Wright on col.12, lines 5-1 and col.14, lines 41-42; discusses recovering the session key from the transformed document and decrypting the transformed document with the session key to recover the original document.

As per claim 4: See Wright on col.13, line 51; discusses applying the private key corresponding to the selected recipient.

As per claim 5: See Wright on col.5, lines 45-56; discusses an encryption step is a combination of a symmetric private key encryption scheme and an asymmetric public key encryption scheme.

As per claim 6: See Wright on col.5, lines 45-56; discusses the asymmetric public key encryption scheme is based on the ElGamal encryption scheme.

As per claim 7: See Wright on col.7, lines 3-5 and col.11, lines 10-11; discusses the encrypted document comprises a first portion representative of the original document encrypted via the symmetric private key encryption scheme using the session key, and a second portion representative of the session key encrypted using an owner's private key according to the asymmetric public key encryption scheme **(col.7, lines 20-21)**.

As per claim 8:

Wright discloses the original document is distributed to the selected recipient through at least one additional intermediate grantor by repeating the following steps for each additional intermediate grantor:

generating a new proxy key based on the intermediate grantor's public key; and **[col.14, lines 65-67]** transforming the encrypted document with the new proxy key to create a transformed document customized for the intermediate grantor. **[col.13, lines 50-51]**

As per claim 10: See Wright on col.7, lines 3-5 and col.11, lines 10-11; discusses the encrypted document comprises a first portion representative of the original document encrypted via the symmetric private-key encrypted scheme using the session key, and a second portion representative of the session key encrypted using an owner's private key according to the asymmetric public-key encryption scheme.

As per claim 11: See Wright on col.5, lines 45-56; discusses encrypted with the modified ElGamal encryption scheme.

As per claim 12: See Wright on col., lines; discusses generating a session key **[col.11, lines 46-50]**, encrypting the original document **[col.5, lines 21-22 and col.7, lines 12-13]**, generating a proxy key **[col.10, lines 26-28 and col.11, line 11]**, transforming the encrypted document are performed by the grantor **[col.12, lines 55-56 and col.14, lines 65-67]**

As per claim 13:

Wright, et al. disclose a system operable to encrypt an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising:

a session key generation system that generates a session key based on a random number **[col.11, lines 46-50]** privately maintained by only the owner, including the encryptor **[col.9, lines 51-52]**, of the original document; **[col.5, lines 2-4 and col.7, lines 10-11]** an encryption system that encrypts the original document with the session key to create an encrypted document; **[col.5, lines 21-22 and col.7, lines 12-13]**

a proxy key generation system that generates a proxy key based on a public key **[col.10, lines 26-28 and col.11, line 11]** corresponding to the selected recipient; and **[col.11, lines 65-67 and col.14, lines 35-36]**

a transformation system that transforms the encrypted document with a proxy key to create a transformed document **[col.14, lines 65-67]**, wherein the encrypted document remains in an encrypted state **[col.12, lines 55-56]** during the transformation to the transformed document.

Wright discloses alternative methods for secure message transmission. There is a method that decrypts and then re-encrypts the message and there is the alternative method of a straight through process of the encryption and the re-encryption process throughout the transformation of the encrypted document where the encryption remains encrypted **[col.13, lines 49-65 and col.14, lines 16-30]**. It is obvious that a message being encrypted is considered a message that has been transformed. However, Wright did not explain the encrypted message transforms to the encrypted message into a transformed message that is not decrypted to the original message and re-encrypted.

Jakobsson teaches proxy cryptography and demonstrates that asymmetric proxy transformations exist (col.3, lines 18-21). Jakobsson discloses the asymmetric encryption where the transformation is performed under quorum control which guarantees that if there is not a dishonest quorum, then the plaintext message whose encryption is being transformed is not revealed to the proxy servers. Jakobsson's solution is efficient allowing tight control over actions and forwarding secret key encrypted messages from a primary recipient to a secondary recipient without disclosing the underlying encrypted message (col.3, lines 50-63). Jakobsson discloses the proxy transforming encrypted messages to encryptions with a variety of different recipient public keys to allow for categorization of the encryptions (col.4, lines 17-20). Further, Jakobsson includes the proxy to transform an encryption which the proxy could not decrypt into an encryption for which the proxy holds the secret key (col.6, lines 10-14). It would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of Wright with transforming the encrypted message to a transformed message that is not decrypted and re-encrypted as taught by Jakobsson because during transformation the plaintext is not revealed which leads to not being decrypted and transforming an encrypted message is efficient and does not disclose the underlying encrypted message (col.3, lines 50-63).

As per claim 14: See Wright on col.14, lines 65-67; discusses transmitting system that transmits the transforming the transformed document to the selected recipient.

As per claim 15: See Wright on col.12, lines 5-1 and col.14, lines 41-42; discusses a recovering system that recovers the session key from the transformed document and decrypting system that decrypts the transformed document with the session key to recover the original document.

As per claim 16: See Wright on col.13, line 51; discusses the recovery of the session key is performed by applying the private key corresponding to the selected recipient.

As per claim 17: See Wright on col.5, lines 45-56; discusses the encryption is performed with a combination of a symmetric private key encryption scheme and an asymmetric public key encryption scheme.

As per claim 18: See Wright on col.5, lines 45-56; discusses the asymmetric public key encryption scheme is based on the ElGamal encryption scheme.

As per claim 19: See Wright on col.7, lines 3-5 and col.11, lines 10-11; discusses the encrypted document comprises a first portion representative of the original document encrypted via the symmetric private key encryption scheme using the session key, and a second portion representative of the session key encrypted using an owner's private key according to the asymmetric public key encryption scheme **(col.7, lines 20-21)**.

As per claim 20: See Wright col.14, lines 65-67 and col.13, lines 50-51; discloses the original document is distributed to the selected recipient through at least one additional intermediate grantor by repeating the following steps for each additional intermediate grantor by using the proxy key generation system to generate a new proxy key based on the intermediate grantor's public key and using the transformation system to transform the encrypted document with the new proxy key to create a transformed document customized for the intermediate grantor.

As per claim 22: See Wright on col.5, lines 45-56; discusses encrypted with the modified ElGamal encryption scheme.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 9 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over the Wright and Jakobsson combination, and in further view of Irish Times "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" (City Edition).

As per claim 9:

Wright discloses a public- private encryption method wherein uses private keys and public keys for encryption and decryption (col.7, lines 59-65). Jakobsson teaches proxy cryptography and demonstrates that asymmetric proxy transformations exist (col.3, lines 18-21). However, the Wright and Jakobsson combination does not include the Cramer-Shoup encryption scheme.

The Irish Times disclosed in its article "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" a Cramer-Shoup encryption scheme **[paragraph 4]** where this encryption was developed by mathematicians from IBM and Swiss Federal Institute of Technology to have created an unbreakable protection for computer data **[paragraph 2]**. Cramer-Shoup method thwarts attacks of decoding encrypted messages passing through the network with bogus messages by adding another series of calculations which ensure the server leaks no information when responding to the bogus text **[paragraph 6]**.

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of the Wright and Jakobsson combination with Cramer-Shoup encryption scheme as taught by The Irish Times because this method thwarts attacks of decoding encrypted messages passing through the network with bogus messages by adding another series of calculations which ensure the server leaks no information when responding to the bogus text.

As per claim 21:

Wright discloses a public- private encryption method wherein uses private keys and public keys for encryption and decryption (col.7, lines 59-65). Jakobsson teaches proxy cryptography and demonstrates that asymmetric proxy transformations exist (col.3, lines 18-21). However, the Wright and Jakobsson combination does not include the Cramer-Shoup encryption scheme.

The Irish Times disclosed in its article "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" a Cramer-Shoup encryption scheme **[paragraph 4]** where this encryption was developed by mathematicians from IBM and Swiss Federal Institute of Technology to have created an unbreakable protection for computer data **[paragraph 2]**. Cramer-Shoup method thwarts attacks of decoding encrypted messages passing through the network with bogus messages by adding another series of calculations, which ensure the server, leaks no information when responding to the bogus text **[paragraph 6]**.

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Wright & Ellison with Cramer-Shoup encryption scheme as taught by The Irish Times because this method thwarts attacks of decoding encrypted messages passing through the network with bogus messages by adding another series of calculations which ensure the server leaks no information when responding to the bogus text.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100